NMCI: The Silver Lining

Subject Area General

EWS 2006

NMCI: The Silver Lining
EWS Contemporary Issue Paper
Submitted by Captain LE Wilson
To
Major Uecker, CG 7
February 2006

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **FEB 2006**	2. REPORT TYPE	3. DATES COVERED **00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE **NMCI: The Silver Lining**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Marine Corps University Library ,2040 Broadway Street ,Quantico,VA,22134**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**15**	

Since the programs inception in 1999, the Navy and Marine Corps Intranet (NMCI) has soured many users across the Department of the Navy (DON). On October 6, 2000 the NMCI contract was awarded to Electronic Data System (EDS) and, five years later, they are still only seventy five percent complete with fielding systems.[1] Users that have been converted have complained of slow service and problems incorporating older software. Despite user-frustration with the implementation and incompatibility issues of the new system, NMCI has been successful in improving network security, providing greater interoperability and providing valuable lessons learned for the Marine Corps.

Background

In the spring of 1999 the Navy and the Marine Corps briefed the Secretary of the Navy on their plans to improve their Information Technology (IT) infrastructure. At the time this brief was presented, the Marine Corps had a contiguous, self-contained network that included all of its bases in the Continental United States (CONUS), Hawaii and Okinawa. These bases were centrally controlled by what is now known as the Marine Corps Network Operations and

[1] Frank Tiboni, “Navy Marine Corps Intranet 75 percent done,” Federal Computer Week, 18 November 2005, <http://www.fcw.com/article91482-11-18-05-Web> (21 November 2005).

Security Command (MCNOSC or legacy network). In contrast, the Navy's infrastructure was neither centrally managed nor controlled. Each Naval base was treated as a local asset, using whatever network design, hardware and software the local authority approved. When the Secretary of the Navy decided that the best move for the DON was to create one enterprise network,[2] the program was outsourced to EDS. The decision to outsource was the result of consulting with the top IT leaders within the DON and with a research development and acquisitions team. These teams and leaders determined that the project would be too expensive to be done internally and that the program should be outsourced. The contractor from whom DON would buy voice, video and data services would also provide the hardware, software, and connectivity. EDS' biggest contribution to the new enterprise network has been increased security.

Network Security

Network Security is the means used to prevent unauthorized access to the local or wide area network. NMCI has taken several steps to improve security. They have by reduced the number of entry points, changed the way

[2] "NMCI yesterday, today and tomorrow," Navy Marine Corps Intranet, <http://www.nmci.navy.mil/Press_Room/Media_Updates_Folder/Media_Update_Items/Yesterday_Today> (18 November 2005).

updates are performed and developed a closer working relationship with the Defense Information Systems Agency (DISA). In a November 18, 2005 article, Federal Computer Weekly quoted a Navy report stating that NMCI security improvements have stopped ten million unauthorized access attempts and quarantined and disinfected sixty thousand viruses this year.[3] Prior to NMCI, the Marine Corps had numerous entry points, known as Points of Presence (POP,) spread across the network. These POPs were regulated and monitored by the MCNOSC and managed by the individual owning units. DISA provided guidance and security requirements to MCNOSC who, in turn, enforced these regulations upon the individual commands. This was managed by the improvements made by NMCI regarding security. The first step to improved security was the consolidation of entry points to what are now four hubs: Norfolk, VA; Quantico, VA; San Diego, CA; Oahu, HI. By reducing the number of entry points NMCI gained greater control and visibility over the traffic that comes in and out of the network, as well as greater ability to respond to and communicate threat activity. Each of these hub sites also has a DISA representative on site to improve communication

[3] Tiboni, “Navy Marine Corps Intranet 75 percent done,” <http://www.fcw.com/article91482-11-18-05-Web>.

of security requirements and help guide actions concerning the network.

Security updates are performed in a more efficient manner under NMCI as well. Under the legacy system the MCNOSC would contact each command and inform them of the new Information Assurance Vulnerability Alerts (IAVA) sent out by DISA. The notice would include a required compliance and report date. However, because not all commands operated a help desk or monitored the network around the clock, there were times when the IAVA would get lost in the work load and would not be completed until follow up contact was made by the MCNOSC. The solution NMCI provides is a 24-hour help desk and automatic loading of patches when computers are logged on. In the event that a patch must be manually loaded an NMCI response team, which are located at every base, can be sent out to reply to problems or apply patches. These capabilities ensure that vulnerabilities are always handled in a timely manner, limiting the time a threat has to cause damage to the network or to exploit a known weakness.

The most significant way NMCI has improved local security is in its ability to exercise security restrictions. Pre-NMCI if a commander desired access to software or assets that would allow for a vulnerability to be exploited, he could direct that access be given to him to receive those assets. The commander's actions would provide an exploitable gap in the defense of the network. Even though this only occurred under extreme circumstances using the legacy network, it is not possible at all under NMCI.

Improved Interoperability

One of the major goals the Secretary of the Navy set when establishing NMCI was to combine the DON under one interoperable enterprise network. Interoperability is defined as the ability to communicate between two different levels or services. NMCI has made strides toward this end by creating the enterprise network and standardizing hardware and software. The enterprise network established by NMCI provides standardization and interoperability between the Navy and Marine Corps and sets the stage for interoperability between other services as well. In the five years it has been in development, NMCI has converted 260,000 of the 346,000 required computers to NMCI.[4] Once an NMCI account has been made, a Marine can travel to any location converted to NMCI and log onto the Marine Corps

[4] Tiboni, "Navy Marine Corps Intranet 75 percent done," <http://www.fcw.com/article91482-11-18-05-Web>.

Domain Service United States (MCDSUS). Once logged on, the Marine will note that the system is interoperable and that all services not dependent on a local hard drive are accessible.

Along with an interoperable enterprise network, NMCI is working with the Marine Corps to standardize software. When the NMCI conversion began, the Marine Corps had close to one thousand legacy applications running. From the stand point of interoperability, the use of so many software applications is unsupportable. By eliminating useless software and allowing only approved software on the network, NMCI has continued the surge toward software standardization and interoperability. EDS has been working with the Marine Corps to manage these programs while gradually increasing requirements to weed out the old legacy applications and move toward a more standardized software package. In the meantime, applications that do not meet standards and requirements are placed in quarantine until they are phased out or converted to an approved application.

Since NMCI owns all of the hardware and software licenses used on the network, they are also responsible to keep this equipment current with industry standards. To stay current, NMCI is responsible for conducting a hardware refresh every three years.[5] This not only not only ensures that changes within the DOD and DON are supported, but it also ensures that hardware will continue to support the latest applications and continues to support the intent of interoperability.

Lessons Learned

The Marine Corps thinks so highly of lesson learned that they have established a center to gather, disseminate, and archive all lesson learned developed. With over 500,000 users, NMCI is the biggest outsourced network in the military, and as a result, its integration has provided for many valuable lessons learned that should be garnered by the Marine Corps and other external agencies.[6]

One of the biggest lessons learned was that of Due Diligence. The web page "www.answers.com", describes Due Diligence as confirming material and facts before a sale.[7] This applies to EDS and the Marine Corps in the context of legacy applications. When EDS was awarded the NMCI contract, they conducted surveys inquiring about the legacy

[5] Joseph Ciprano, "What NMCI Means to Us," CHIPS magazine, <http://www.chips.navy.mil/archives/01_nmci/cipriano.htm> (18 November 2005).

[6] Tiboni, "Navy Marine Corps Intranet 75 percent done," <http://www.fcw.com/article91482-11-18-05-Web>.

[7] "Due Dilligence" answers.com, <http://www.answers.com/topic/due-diligence> (15 December 2005).

applications running on the legacy network. EDS failed to capture the entire scope of legacy applications impart due to the lack of support that was received from the Marine Corps. In many cases applications were running on the legacy network with almost total autonomy or with only one or two individuals managing the applications. This situation only became prevalent when the conversions began and the discrepancies were noticed. The result is quarantined software that requires a separate network to be maintained. This means that many DON employees who have been converted to NMCI must have two computers to effectively do their jobs. One computer runs NMCI approved applications and software the other computer runs unsupported legacy applications. If more attention to detail had been given to what programs were running and what support would be required, the problem with legacy applications could have been better prepared for and mitigated.

The procurement process for acquiring outsourced services and products need to be closely considered as a lesson learned as well as another example of Due Diligence. Once it has been determined that a service or product will be purchased, a lengthy process of advertising and bidding is done before a contract is awarded. EDS was not the only bidder for the contract, but they were the lowest bidder. A fact that was sure to have played a role in them being awarded the contract. EDS actually underbid the true value of the contract though and operated with negative cash flows for the first three years of service. They were basically unprepared for what they were hired to do, and as a result, the transition has taken longer than expected and met with more difficulties along they way.[8]

Finally, it is important to understand that major cultural changes such as the outsourcing of NMCI will have on military members. Because outsourcing involves “taking away” tasks that were previously performed by government employees and military members, it is usually greeted with resistance that can slow the process down. However, implementing a performance-based alternative where both the contractor and military organization mutually benefit and appreciate the value of achieving common goals, will help alleviate potential tension.

The lessons learned from outsourcing the entire DON IT infrastructure has had a significant affect on the way business is conducted within the DON and especially the

[8] Dawn Onley, “Hanlon on NMCI ‘EDS was not prepared’,” Government Computer News, 22 June 2004, <http://www.gcn.com/vol1_no1/daily-updates/26324-1.html> (16 November 2005).

Marine Corps. This bears noting for the benefit of future outsourced projects.

Conclusion

NMCI began as an idea by the Secretary of the Navy as a way of improving the IT infrastructure within the DON. Since then, NMCI has been a sore spot across the Marine Corps. There have been, however, some improvements. The DON's networks are now more secure as a result of consolidating entry points and the timeliness and efficiency of employing security. Under NMCI, the Marine Corps is standardizing hardware and software to facilitate interoperability within the DON and with the other services. Finally, there have been valuable lessons learned from outsourcing NMCI, such as, the application of due diligence and the importance of knowing what is required and expected from both parties. NMCI certainly was not welcome by the Marine Corps, but Marines always make the best of what they have available.

Word Count 1826

BIBLIOGRAPHY

1. “$9 billion Bugs for U.S. Navy-Marine Corps Intranet June 22, 2005,” Prescient Digital Media, 22 June 2005, <http://www.prescientdigital.com/Services/Intranets/IntranetBlog/June_2005_IntranetBlog/nine_billion_bugs.htm> (15 November 2005).
2. Browne, Herbert, “Interoperability flows from the top,” Signal Magazine, April 2004, <http://www.afcea.org/signal/articles/anmviewer.asp?a=81&z=35> (18 November 2005).
3. Carr, David, “Half-Speed,” Find Articles, April 2004, <http://www.findarticles.com/p/articles/mi_zdbln/is_200404/ai_ziff123704> (15 September 2005).
4. Cipriano, Joseph, “NMCI Update,” Connecting Technology, 17 May 2001, <http://www.chips.navy.mil/archives/01_summer/nmci_update.htm> (16 November 2005).
5. Cipriano, Joseph, “What NMCI Means to Us,” CHIPS magazine, <http://www.chips.navy.mil/archives/01_nmci/cipriano.htm> (18 November 2005).

6. Connolly, Allison, “Military’s intranet under fire,” The Virginian Pilot” 22 June 2005, <http://home.hamptonroads.com/stories/story.cfm?story=88142&ran=39753> (15 November 2005).

7. “Due Diligence,” answers.com, <http://www.answers.com/topic/due-diligence> (15 December 2005).

8. Gerber, Cheryl, “NMCI: Now For the Networks,” Military Information Technology, 31 December 2003, <http://www.military-information-technology.com/article.cfm?DocID=346> Volume: 7 Issue: 10, (18 November 2005).

9. Jadegold, “Questions and Answers,” May 2005, <http://qando.net/archives/002909.htm> (18 November 2005).

10. Kennedy, Harold, “Taking Fire, Navy Marine Corps Intranet Progress,” National Defense, November 2003, <http://www.nationaldefensemagazine.org/issues/2003/Nov/Taking_Fire.htm> (17 November 2005).

11. Lawlor, Maryann, “Enterprise Network Deploys Overseas,” Signal Magazine, March 2005, <http://www.afcea.org/signal/articles/anmviewer.asp?a=691> (18 November 2005).

12. “NMCI Announces Second Quarter 2005 Customer Satisfaction Survey Results,” Navy Marine Corps Intranet, <http://www.fcw.com/article91482-11-18-05-Web> (25 November 2005).

13. “NMCI gets hacked,” White Dust Solutions, 15 November 2005, <http://www.whitedust.net/newsview.php?NewsID=1625> (18 November 2005).

14. “NMCI yesterday, today and tomorrow,” Navy Marine Corps Intranet, <http://www.nmci.navy.mil/Press_Room/Media_Updates_Folder/Media_Update_Items/Yesterday_Today> (18 November 2005).

15. “Navy-Marine Corps Announce Intranet Contract Award,” Defense Link News, 6 October 2000, <http://www.defenselink.mil/releases/2000/b10062000_bt618-00.html> No. 618-00, (14 September 2005).

16. “Navy Marine Corps Intranet,” EDS, <http://www.eds.com/sites/nmci/> (18 November 2005).

17. Onley, Dawn, “Hanlon on NMCI ‘EDS was not prepared’,” Government Computer News, 22 June 2004, <http://www.gcn.com/vol1_no1/daily-updates/26324-1.html> (16 November 2005).

18. Onley, Dawn S., “Other agencies could benefit from NMCI’s hard-learned lessons,” Government Computer Weekly, 20 June 2005, <http://www.gcn.com/24_15/dodcomputing/36091-1.html> (15 September 2005) vol. 24 no.15.

19. Tiboni, Frank, “Navy Marine Corps Intranet 75 percent done,” Federal Computer Week, 18 November 2005, <http://www.fcw.com/article91482-11-18-05-Web> (21 November 2005).

20. Webb, Cynthia, “Navy-Marine Corps Project Takes Fresh Flak,” The Washington Post, 24 June 2004, <http://www.washingtonpost.com/wp-dyn/articles/A2854-2004Jun24.html> (16 November 2005).